2

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-268075
(43)Date of publication of application : 28.09.2001

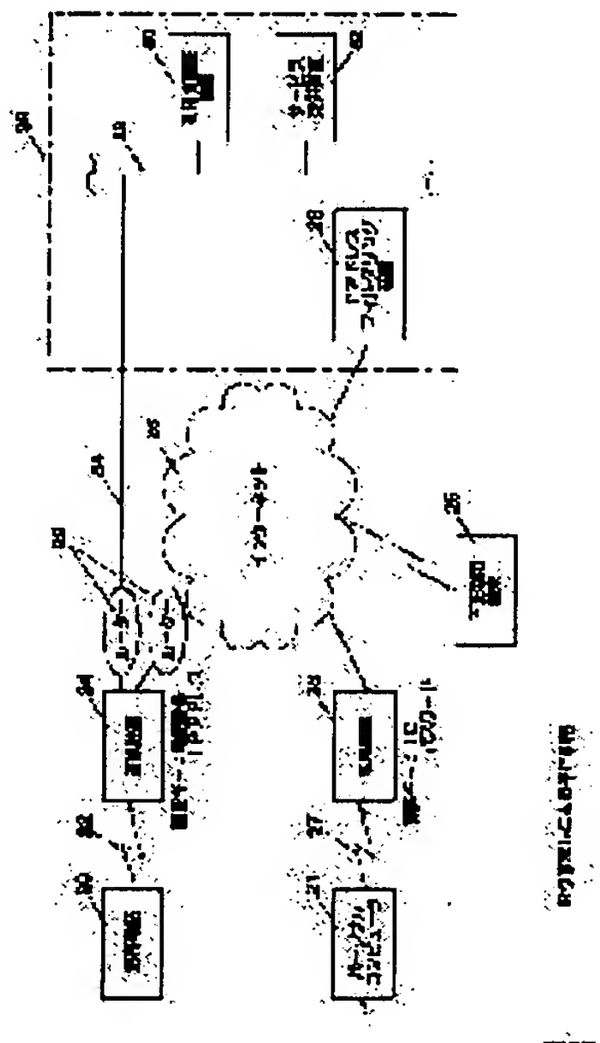
(51)Int.CI. H04L 9/32
G06F 15/00
H04Q 7/38

(21)Application number : 2000-075555
(22)Date of filing : 17.03.2000

(71)Applicant : KYOCERA COMMUNICATION SYSTEMS CO LTD
(72)Inventor : MIYAHIRO EIICHI
OSAKO TETSUO

(54) USER AUTHENTICATION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a user authentication system that can prevent unauthorized use.
SOLUTION: When a mobile phone 20 receives provision of a service of a service provision unit 32, a telephone number and an IP address as an authentication key sent from the mobile phone 20 are transmitted to a user authentication unit 30 via the Internet 26 or a leased line 34. An IP address filtering unit 28 receiving the authentication key via the Internet 26 does not transmit the authentication key to the user authentication unit 30 if the authentication key includes an IP address given by a converter 24. The authentication key sent via the leased line 34, on the other hand, is transmitted to the user authentication unit 30, which authenticates the user. Even when an unauthorized user tries to unauthorizedly use the system in a way of a pretended mobile phone user by acquiring the authentication key transmitted through the Internet 26, the IP address filtering unit 28 does not transmit the authentication key to the user authentication unit 30.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision

of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2001－268075
(P2001－268075A)
(43)公開日　平成13年９月28日(2001.9.28)

(51)Int.Cl.⁷	識別記号	ＦＩ	テーマコード(参考)
Ｈ０４Ｌ　9/32		Ｇ０６Ｆ　15/00	３３０Ｃ　５Ｂ０８５
Ｇ０６Ｆ　15/00	３３０	Ｈ０４Ｌ　9/00	６７３Ｂ　５Ｊ１０４
Ｈ０４Ｑ　7/38		Ｈ０４Ｂ　7/26	１０９Ｒ　５Ｋ０６７

審査請求　未請求　請求項の数８　ＯＬ　（全 12 頁）

(21)出願番号　特願2000－75555(P2000－75555)

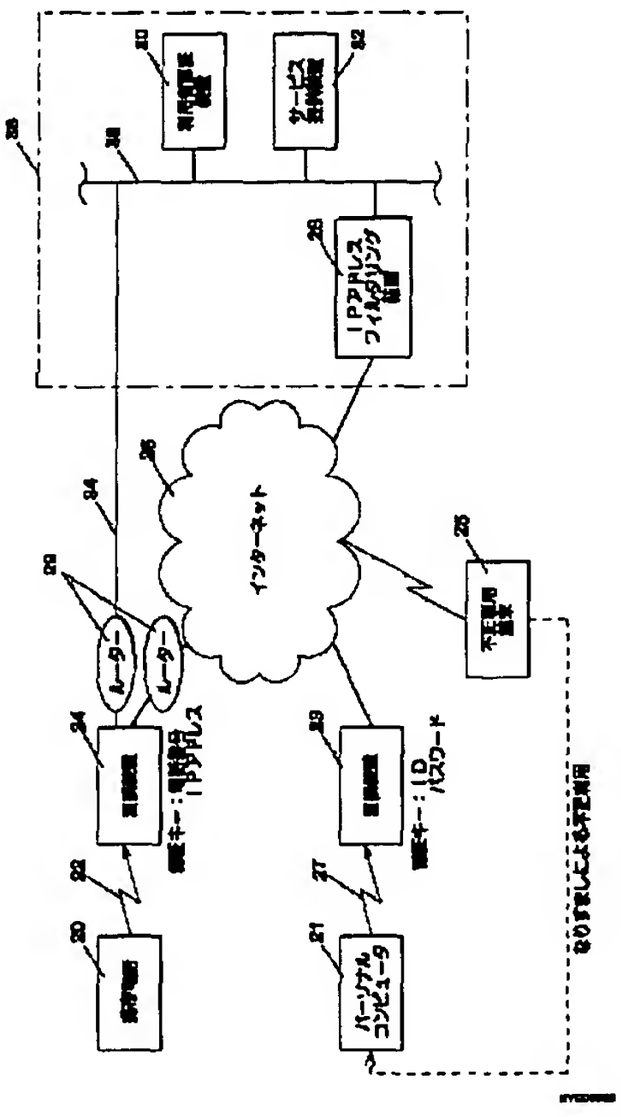
(22)出願日　平成12年３月17日(2000.3.17)

(71)出願人　596100812
京セラコミュニケーションシステム株式会社
京都市山科区東野北井ノ上町５番地の22
(72)発明者　宮廣　栄一
京都府京都市山科区東野北井ノ上町５番地の22　京セラコミュニケーションシステム株式会社内
(74)代理人　100092956
弁理士　古谷　栄男　（外２名）

最終頁に続く

(54)【発明の名称】　利用者認証システム

(57)【要約】
【課題】　不正利用を防止することのできる利用者認証システムを提供する。
【解決手段】　携帯電話２０によって、サービス提供装置３２のサービスの提供を受ける場合、携帯電話２０から送信された認証キーとしての電話番号とIPアドレスは、インターネット２６または専用線３４を介して利用者認証装置３０に向けて送信される。インターネット２６経由中で認証キーを受信するIPアドレスフィルタリング装置２８は、その認証キーが変換装置２４で付与されたIPアドレスを含んでいれば、その認証キーを利用者認証装置３０に送信しない。一方、専用線３４経由で送信された認証キーは送信されて利用者認証が行われる。インターネット２６上を流れるその認証キーを取得することにより携帯電話へのなりすまし不正利用をしても、IPアドレスフィルタリング装置２８はその認証キーを利用者認証装置３０に送信しない。



【特許請求の範囲】
【請求項１】端末装置、
端末装置に対して専用線を介して接続された識別情報付加装置、
識別情報付加装置に対して通信路を介して接続された識別情報選択送信装置、
識別情報付加装置に対して専用線を介して接続されるとともに識別情報選択送信装置に対しても専用線を介して接続された利用者認証装置、
を備えた利用者認証システムであって、
端末装置は、
識別情報付加装置に対して利用者情報を送信する利用者情報送信手段を備え、
識別情報付加装置は、
端末装置から送信された利用者情報に対して識別情報を付加する識別情報付加手段と、
識別情報付加手段によって得られた利用者識別情報を通信路を介して識別情報選択送信装置に向けて送信する通信路経由利用者識別情報送信手段と、
前記利用者識別情報を専用線を介して利用者認証装置に対して送信する専用線経由利用者識別情報送信手段とを備え、
識別情報選択送信装置は、
識別情報付加装置が付加する識別情報を含んだ利用者識別情報は利用者認証装置に送信しないが前記識別情報以外の識別情報を含んだ利用者識別情報は利用者認証装置に送信する利用者識別情報選択送信手段を備え、
利用者認証装置は、
識別情報付加装置または識別情報選択送信装置から専用線を介して送信される利用者識別情報を受けて利用者認証を行う利用者認証手段、
を備えたことを特徴とする利用者認証システム。
【請求項２】請求項１の識別情報付加装置において、さらに、
利用者識別情報を通信路を介して識別情報選択送信装置に向けて送信するかまたは専用線を介して利用者認証装置に対して送信するかのいずれかを選択する送信経由選択手段、
を備えたことを特徴とするもの。
【請求項３】識別情報付加装置に対して通信路を介して接続されるとともに、利用者認証装置に対して専用線を介して接続された識別情報選択送信装置において、
識別情報付加装置が付加する識別情報を含んだ利用者識別情報は利用者認証装置に送信しないが前記識別情報以外の識別情報を含んだ利用者識別情報は利用者認証装置に送信する利用者識別情報選択送信手段、
を備えたことを特徴とする識別情報選択送信装置。
【請求項４】請求項１～３のいずれかの識別情報選択送信装置において、さらに、
識別情報付加装置が付加する識別情報を記憶した記憶部、

を備えており、
識別情報選択送信手段は、前記記憶部を参照することによって、利用者認証装置に送信する利用者識別情報と送信しない利用者識別情報とを選択することを特徴とするもの。
【請求項５】請求項４の利用者認証システムにおいて、
識別情報付加装置が付加する識別情報が更新された場合には、
識別情報付加装置は、さらに、
更新された識別情報を専用線を介して識別情報選択送信装置に対して送信する更新識別情報送信手段を備え、
識別情報選択送信装置は、さらに、
前記記憶部の更新を前記送信された更新識別情報に基づいて行う選択送信識別情報更新手段、
を備えたことを特徴とする利用者認証システム。
【請求項６】請求項１～５のいずれかの利用者認証システムにおいて、
識別情報選択送信装置と利用者認証装置が一体の装置として構成されていることを特徴とする利用者認証システム。
【請求項７】請求項１～６において、
識別情報は、IPアドレスであることを特徴とするもの。
【請求項８】端末装置の利用者を、端末装置に接続された利用者認証装置によって認証する利用者認証方法であって、
端末装置が利用者認証を受ける際には、
端末装置からの利用者情報に識別情報を付加して、通信路または専用線経由により利用者認証装置に向けて送り、
通信路経由により送られた前記識別情報を有する利用者情報は利用者認証装置に送られず、専用線経由により送られた利用者情報は利用者認証装置に送られ、
利用者認証装置は、専用線経由により送られた前記利用者情報に基づいて利用者認証を行う利用者認証方法。
【発明の詳細な説明】
【０００１】
【発明の技術分野】この発明はインターネットなどのネットワークを用いてサービスを提供するサービスシステムにおける利用者認証に関するものであり、特に、不正利用防止に関する。
【０００２】
【従来の技術】図１に、インターネットを利用した従来の利用者認証システムを示す。利用者端末２は、インターネット利用可能な携帯電話やパーソナルコンピューター等である。利用者端末２は、電話網１４を介して変換装置４に接続されており、変換装置４は、インターネット６に接続されている。そして、インターネット６には、利用者認証装置８とサービス提供装置１０がそれぞれ接続されており、利用者認証装置８とサービス提供装

置１０はLAN１６で接続されている。

【０００３】利用者端末２がサービス提供装置１０のサービスを利用するにあたっては、その前提として利用者認証を行う必要がある。このため、利用者端末２は、まず、利用者端末２を特定するための識別子を変換装置４に送信する。それを受けた変換装置４は、ネットワーク上で利用者端末を一意に特定するために、利用者端末２に対するIPアドレスの配布と、送信された識別子にIPアドレスを付与したものである認証キーを、電話網からインターネットへのプロトコル変換を行う。そして、変換装置４は、認証キーをインターネット６を介して利用者認証装置８に送信する。その認証キーを受けた利用者認証装置８は、利用者認証を行い、認証が終了した後にはサービス提供装置１０が利用者端末２に対してサービスの提供を行う。すなわち、利用者認証装置８は、利用者端末２から送られてくる認証キーが真正なものでなければ利用者の認証を拒否し、真正のものであればサービス利用を許可する。

【０００４】ここで、利用者端末としては、インターネット利用可能な携帯電話やパーソナルコンピューター等の仕様が異なる様々なものが存在する。したがって、そのような種々の利用者端末から同じ情報にアクセスする場合を考慮した結果として、利用者認証装置はインターネット経由ですべてのアクセスを取り扱うのが好ましいと考えられる。

【０００５】一方、利用者端末がパーソナルコンピューターの場合は、認証キーとしてパスワードやID が用いられるのが一般的であるが、インターネット利用可能な携帯電話の場合は利用者の操作簡便化のため電話番号により一意に特定される加入者IDが用いられることがある。

【０００６】

【発明が解決しようとする課題】しかしながら、従来の利用者認証システムには次のような問題があった。

【０００７】パーソナルコンピューターが認証キーとして送信するパスワードやIDと比較すると、インターネット利用可能な携帯電話が認証キーとして送信する電話番号により一意に特定される加入者IDは、偽造が比較的容易な変数としてインターネット上を流れるため、悪意の利用者が、正規の携帯電話の利用者になりすまして不正利用を行う懸念が生じる。

【０００８】すなわち、図１のインターネット６を流れている加入者IDを不正利用端末１２（不正プログラムを備えたパーソナルコンピューター等）により取得した悪意の利用者が、その不正利用端末１２を操作して正規の携帯電話の利用者になりすまして利用者認証装置８にアクセスしてサービスの提供を受けた場合には正規の利用者が不測の損害を被るおそれがある。特にそのサービスが有料である場合には、不正利用をされた利用者が、サービスの提供を受けていないにもかかわらず料金を負担

しなければならないという事態が懸念されるという問題がある。

【０００９】なお、このような問題は、インターネット利用可能な携帯電話と違って、パーソナルコンピューター等は、不正利用者がそのパーソナルコンピューターのプログラムの変更を行うことができる可能性がある、ということを背景としているものである。

【００１０】このような状況は、インターネット利用可能な携帯電話の利用者にとっては不安要因となるものであり、また、今後増加すると予想される、携帯電話によってインターネットを利用したサービスの提供を受けるというシステムの発達を阻害する要因として懸念される。

【００１１】この発明は、上記のような問題に鑑みて、不正利用を防止することのできる利用者認証システムを提供することを目的とする。

【００１２】

【課題を解決するための手段および発明の効果】（１）この発明の利用者認証システムは、端末装置、端末装置に対して専用線を介して接続された識別情報付加装置、識別情報付加装置に対して通信路を介して接続された識別情報選択送信装置、識別情報付加装置に対して専用線を介して接続されるとともに識別情報選択送信装置に対しても専用線を介して接続された利用者認証装置、を備えた利用者認証システムであって、端末装置は、識別情報付加装置に対して利用者情報を送信する利用者情報送信手段を備え、識別情報付加装置は、端末装置から送信された利用者情報に対して識別情報を付加する識別情報付加手段と、識別情報付加手段によって得られた利用者識別情報を通信路を介して識別情報選択送信装置に向けて送信する通信路経由利用者識別情報送信手段と、前記利用者識別情報を専用線を介して利用者認証装置に対しても送信する専用線経由利用者識別情報送信手段とを備え、識別情報選択送信装置は、識別情報付加装置が付加する識別情報を含んだ利用者識別情報は利用者認証装置に送信しないが前記識別情報以外の識別情報を含んだ利用者識別情報は利用者認証装置に送信する利用者識別情報選択送信手段を備え、利用者認証装置は、識別情報付加装置または識別情報選択送信装置から専用線を介して送信される利用者識別情報を受けて利用者認証を行う利用者認証手段、を備えたことを特徴としている。

【００１３】これにより、通信路を流れている利用者識別情報を不正に取得した悪意の利用者が、正規の端末装置の利用者になりすまして利用者認証を受けることを試みた場合でも、利用者認証はされないことになる。

【００１４】なぜならば、悪意の利用者が送信する利用者識別情報は、本発明における識別情報付加装置とは別の経由で通信路に送信されることになるのであるから、専用線経由による送信はされない。さらに、その不正に取得した利用者識別情報に含まれる識別情報は、本発明

における識別情報付加装置が付加する識別情報と同一のものであるから、識別情報選択送信装置はその利用者識別情報を利用者認証装置に送信しないからである。

【００１５】そして、一方の専用線を流れている利用者識別情報は第三者に取得されることがなく、安全に利用者認証装置に送信される。したがって、なりすましによる不正利用を防止することができる。

【００１６】また、通信路と専用線から同じ情報が利用者認証装置に送信されることがないので、利用者識別情報の衝突等といったシステム上の不都合は生じない。

【００１７】さらに、利用者識別情報が偽造容易なものであっても不正利用を防止することができるので、利用者識別情報は簡易なものでよい一方で、端末装置の利用者の操作簡便化が図られるとともに、信頼性の高いシステムが構築できる。

【００１８】また、従来の利用者認証システムに、専用線と識別情報選択送信装置を設けるだけでよいのであるから、構成がシンプルであり低コストで不正利用の防止をすることができる。

【００１９】（２）この発明の識別情報付加装置は、さらに、利用者識別情報を通信路を介して識別情報選択送信装置に向けて送信するかまたは専用線を介して利用者認証装置に対して送信するかのいずれかを選択する送信経由選択手段、を備えたことを特徴としている。

【００２０】これにより、専用線を介して利用者識別情報を利用者認証装置に送信する場合には、利用者識別情報の安全性がより確実に確保される。すなわち、利用者識別情報が通信路上を流れた場合には、第三者が不正にその情報を取得する可能性があるが、専用線のみが経由として選択される場合にはそのような危険性はない。

【００２１】（３）この発明の利用者認証システムの識別情報選択送信装置は、識別情報付加装置が付加する識別情報を記憶した記憶部、を備えており、識別情報選択送信手段は、前記記憶部を参照することによって、利用者認証装置に送信する利用者識別情報と送信しない利用者識別情報とを選択することを特徴としている。

【００２２】したがって、様々な仕様の利用者端末が新たに加わったり、使用されなくなった場合に、識別情報選択送信装置が利用者認証装置に送信しない利用者識別情報の設定や更新を行う際には、記憶部における識別情報の記憶内容の設定や更新のみで対応できる。

【００２３】（４）この発明の利用者認証システムは、識別情報付加装置が付加する識別情報が更新された場合には、識別情報付加装置は、さらに、更新された識別情報を専用線を介して識別情報選択送信装置に対して送信する更新識別情報送信手段を備え、識別情報選択送信装置は、さらに、前記記憶部の更新を前記送信された更新識別情報に基づいて行う選択送信識別情報更新手段、を備えたことを特徴としている。

【００２４】したがって、識別情報選択送信装置が利用者認証装置に送信しない利用者識別情報を、新たに設定する場合だけでなく、端末装置の仕様が異なる様々なものが新たに加わったり減ったりした場合においても、その記憶部の記憶内容の更新を簡易かつ迅速に行うことができる。

【００２５】また、更新された利用者識別情報は専用線のみを介して識別情報選択送信装置に送信されるから情報の安全性が確保される。すなわち、更新された識別情報が通信路上を流れた場合には、それを取得した第三者がその更新情報に変更を加えたり等することにより本システムが正常に機能しないようにされるおそれがあるが、本発明によればそのような危険性はない。

【００２６】（５）この発明の利用者認証システムにおける識別情報は、IPアドレスであることを特徴としている。

【００２７】ここで、IPアドレスは、識別情報付加装置が利用者情報に付加するものであり、コンピューターが管理・理解しやすい数字等によって表されるものであるから、識別情報選択送信装置に記憶させる内容の規格が統一化され、識別情報のデータ更新が容易であるとともに記憶容量を少なくすることができ、識別情報選択送信手段の処理を迅速化することができる。

【００２８】（６）用語の定義

この発明において、「端末装置」とは、サービスの提供を受ける側の装置であって、インターネット等のネットワークに接続可能な装置をいう。実施形態では、図２の携帯電話２０とパーソナルコンピューター２１の利用者端末がこれに該当する。

【００２９】「通信路」とは、無線、有線を問わず、２以上の装置との通信を行うためのものをいい、インターネットのように開放されたものだけでなく、LANのように閉じられたものも含む概念である。実施形態では、図２のインターネット２６がこれに該当する。

【００３０】「専用線」とは、無線、有線を問わず、２以上の装置との通信を行うためのものをいうが、閉じられた回線のみに限定されインターネットのように開放されたものは含まない概念であり、情報通信を行う２点間が閉じられた回線における電話網、LAN等をいう。実施形態では、図２の電話網２２、２７、専用線３４、LAN３６がこれに該当する。

【００３１】「利用者情報」とは、端末装置の利用者を特定するために端末装置から送信される識別子であり、電話番号やID、パスワード、デジタル証明書等をいう。実施形態では、図６のステップＳ１の電話番号がこれに該当する。

【００３２】「識別情報」とは、端末装置から送信される電話番号等の識別子に対して付加される情報であり、ネットワーク上で利用者端末を一意に特定するためのアドレスをいう。実施形態では、図６のステップＳ３のIPアドレスがこれに該当する。

【００３３】「識別情報付加装置」とは、実施形態においては図２の変換装置２３および２４が該当する。

【００３４】「利用者識別情報」とは、端末装置の利用者を特定するために端末装置から送信される識別子に対して、ネットワーク上で利用者端末を一意に特定するためのアドレスが付与された情報をいう。実施形態では、図６のステップＳ５の認証キーがこれに該当する。

【００３５】「識別情報選択送信装置」とは、実施形態においては図２のIPアドレスフィルタリング装置２８が該当する。

【００３６】「送信経由選択手段」とは、実施形態においては図２のルーター２９が該当する。

【００３７】「識別情報付加装置が付加する識別情報を記憶した記憶部」とは、実施形態においては図７のIPアドレスフィルタリングテーブルが該当する。

【００３８】

【発明の実施の形態】（１）利用者認証システムの実施形態の構成

本発明に係る利用者認証システムの実施形態を図面に基づいて説明する。図２に、この発明の一実施形態による利用者認証システムの構成を示す。携帯電話２０とパーソナルコンピューター２１は、利用者端末である。携帯電話２０は、電話網２２を介して変換装置２４に接続されており、パーソナルコンピューター２１は、電話網２７を介して変換装置２３に接続されている。携帯電話２０は、インターネット利用可能であり、パーソナルコンピューター２１は、通常の電話によるダイヤルアップ接続または常時接続によってインターネット利用可能である。つまり、携帯電話２０は変換装置２４を介して、パーソナルコンピューター２１は変換装置２３を介して、それぞれがインターネット２６に接続可能となっている。なお、変換装置２４には、専用線３４またはインターネット２６のいずれかの経由を選択するためのルーター２９が設けられている一方、利用者認証等を行う、IPアドレスフィルタリング装置２８と、利用者認証装置３０、サービス提供装置３２とは、管理センター３８内に設置されており、それぞれの装置は、管理センター３８内のLAN３６によってお互いに接続されている。また、IPアドレスフィルタリング装置２８は、インターネット２６とも接続されており、LAN３６は、専用線３４に接続されている。

【００３９】変換装置２３、２４は、一般的には電話通信事業者によって運営されている。また、管理センター３８は、電話通信事業者などの公共性の高い組織やその認定業者などが運営することが好ましい。

【００４０】（２）パーソナルコンピューター２１等のハードウェア構成

図３に、パーソナルコンピューター２１のハードウェア構成を示す。パーソナルコンピューター２１は、メモリ４０、ディスプレイ４２、通信回路４４、キーボード／マウス４６、CPU４８、ハードディスク（記録装置）５０、CD-ROMドライブ５２を備えている。また、ハードディスク５０には、オペレーティングシステム（マイクロソフト社のWindows98など）、ウェブを閲覧するためのブラウザプログラムが格納されている。このブラウザプログラムは、CD-ROMドライブ５２を介して、CD-ROM５４からインストールされたものである。通信回路４４は、インターネット２６に接続するための回路である。

【００４１】変換装置２３および２４、利用者認証装置３０、サービス提供装置３２も、それぞれ、図３に示すハードウェア構成と同様である。ただし、変換装置２３および２４においては、ハードディスクにIPアドレスとプロトコル変換プログラムが記録されており、利用者認証装置３０においては、ハードディスクに利用者認証プログラムが記録されており、サービス提供装置３２においては、ハードディスクにサービス提供のためのサービス提供ウェブサーバープログラムが記録されている。

【００４２】（３）IPアドレスフィルタリング装置２８のハードウェア構成

図４に、IPアドレスフィルタリング装置２８のハードウェア構成を示す。IPアドレスフィルタリング装置２８は、表示パネル９０、メモリ９２、通信回路９４、スイッチ９６、CPU９８を備えている。通信回路９４は、インターネット２６に接続するための回路である。

【００４３】（４）携帯電話２０の構成

図５に、携帯電話２０のブロック図を示す。入出力デバイスとして、液晶ディスプレイ６２、テンキー／スイッチ６４、マイク６６、スピーカ（通話用）６８、スピーカ（着信音用）７０が設けられている。音声符号化回路７４は、マイク６６からの音声を送信のために符号化し、受信した音声信号を復号化してスピーカ６８から出力するための回路である。マイクロブラウザ７２は、記録装置に記録されたプログラムであって、サービス提供ウェブからのデータを閲覧するためのものである。無線通信回路７６は、音声やデータを無線通信によって送信しまたは受信するための回路である。シリアルデータ通信回路７８は、外部のパーソナルコンピューター８４との通信を行うための回路である。メモリ８０には、利用者自身の電話番号、電話帳などが記録されている。制御回路８６は、これらの回路を制御する。また、バッテリー８２は、各部に電源を供給する。

【００４４】（５）携帯電話２０から利用者認証を受ける場合の処理

図６に、利用者端末としての携帯電話２０から利用者認証を受ける場合の処理を示す。この処理は利用者端末がサービス提供装置３２からサービスの提供を受ける際の前提となるものである。

【００４５】まず、利用者は、携帯電話２０を操作して変換装置２４に接続し、利用者認証装置３０への接続要求と利用者認証のための識別子である電話番号を送信す

る（ステップＳ１）。変換装置２４は、これを受けて接続許可（ステップＳ２）と、電話番号に対するIPアドレスの付与（ステップＳ３）と携帯電話２０に対するIPアドレスの配布（ステップＳ４）を行う。ここで、変換装置２４は、携帯電話２０に対して配布するIPアドレスをあらかじめハードディスクにプールしており、携帯電話２０からの接続要求がある度毎にそのプールしているIPアドレスから空いているものを選択して配布している。

【００４６】そして、識別子である電話番号は、加入者IDに変換されるとともに（ステップＳ５）、電話網からインターネットプロトコルへプロトコル変換される（ステップＳ６）。ここで、加入者IDは、通信事業者が、利用者の電話番号と一意に対応づけて付与している識別子である。そして、認証キーとしての、加入者IDとIPアドレスは、専用線３４とLAN３６を介して利用者認証装置３０に送信される（ステップＳ７）。

【００４７】このとき、変換装置２４は、前記認証キーをインターネット２６には送信しない。これは、変換装置２４に設けられたルーター２９によるものである。すなわち、前記ステップＳ１の接続要求に含まれるあて先のIPアドレスが、利用者認証装置３０やサービス提供装置３２のアドレスであれば、認証キーの送信経由として専用線３４のみを選択するようにルーター２９が設定されていることによる。

【００４８】したがって、携帯電話２０から送信された認証キーは、専用線３４経由（ステップＳ７）のみで利用者認証装置３０に送信されて利用者認証が行われる（ステップＳ１１）。

【００４９】（６）なりすましによる不正利用の防止について

次に、本実施形態の構成により、携帯電話の利用者へのなりすましによる不正利用を防止できることを説明する。

【００５０】ここで、携帯電話の利用者へのなりすましによる不正利用は、正規に利用者認証されるべき携帯電話２０の利用者が本システム以外の他のインターネットサービス等を利用するときに、インターネット２６上に送信されることになる認証キーを、パーソナルコンピューター等の不正利用端末２５を操作する悪意の利用者が取得することによって行われる。つまり、不正利用端末２５を操作する悪意の利用者は、インターネット２６上を流れる認証キーとしての加入者IDとIPアドレスを、不正利用端末２５内の不正プログラムによって取得・解読する。そして、パーソナルコンピューター等の不正プログラムにより、あたかもその取得した加入者IDとIPアドレスが発信元であるかのようになりすまして変換装置２３にアクセスをし、変換装置２３から本来割り当てられるIPアドレスとは異なるIPアドレスとして、不正にインターネットに侵入すること等によって行われる。

【００５１】しかし、そのようなりすましの不正利用によるサービスの提供を受けることを試みた場合でも、その認証キーは利用者認証装置３０には送信されない。

【００５２】これは、以下に説明するIPアドレスフィルタリング装置２８の構成によるものである。

【００５３】IPアドレスフィルタリング装置２８は、送信された認証キーを受けてフィルタリングを行う。これは、IPアドレスフィルタリング装置２８のメモリ９２に記憶されている、図７に例示するようなIPアドレスフィルタリングテーブルを参照して行うものである。

【００５４】図７のIPアドレスフィルタリングテーブルには、Reject（禁止）のAction をする場合の、発信元のIPアドレスのカラムが記録されており、このIPアドレスは変換装置２４がプールしているIPアドレスと同一である。このReject（禁止）のAction は、認証キーがインターネット２６から送信された場合、その認証キーがカラムに記録されたものと同一のIPアドレスを含んでいれば、その認証キーを利用者認証装置３０に送信しないという動作を行わせるものである。例えば、図７のIPアドレスフィルタリングテーブルにおいては、認証キー中の発信元のIPアドレスが、192.168.1.5であればその認証キーは利用者認証装置３０には送信されない。一方、認証キー中の発信元のIPアドレスが、193.100.1.1であればその認証キーは利用者認証装置３０に送信されることになる。

【００５５】これにより、パーソナルコンピュター等による携帯電話の利用者へのなりすましの不正利用で認証キーを送信しても、それを受ける変換装置２３はその認証キーをインターネット２６のみを経由として利用者認証装置３０に向けて送信する一方で、その認証キーは、IPアドレスフィルタリングテーブル中に記録されている、本来携帯電話２０に割り当てられるIPアドレスを含んでいるため、それを受信したIPアドレスフィルタリング装置２８はその認証キーを利用者認証装置に送信しない（ステップＳ９）。すなわち、利用者認証はされないことになる。

【００５６】（７）本実施形態による効果について

以上のように、本実施形態によれば、パーソナルコンピューター等による携帯電話の利用者へのなりすましの不正利用を防止することができる。

【００５７】また、インターネット２６と専用線３４から同じ情報が利用者認証装置３０に送信されることがないので、IPパケットの衝突等といったシステム上の不都合は生じない。

【００５８】さらに、利用者認証のために送信する情報が加入者IDやIPアドレスである場合のように比較的偽造容易なものであっても不正利用がされないので、特別に携帯電話を操作してパスワードを送信する等の手間の必要がなく利用者の操作簡便化が図られるとともに、信頼性の高いシステムが構築できる。

【００５９】そして、従来の利用者認証システムに専用

線とIPアドレスフィルタリング装置を設けるだけでよいのであるから、構成がシンプルであり低コストで不正利用の防止ができる。

【００６０】さらに、変換装置２４に設けられたルーター２９により、専用線３４が経由として選択された場合には認証キーの安全性がより確実に確保される。すなわち、認証キーがインターネット２６上を流れた場合には、第三者が不正にその認証キーを取得する可能性があるが、専用線３４のみが経由として選択される場合にはそのような危険性はない。

【００６１】なお、専用線３４が経由として選択されて利用者認証がされた場合に、利用者認証終了後の携帯電話２０に対する情報の送信を行う経路としては管理センター３８内の専用線３４を使用するのが通常である。かかる場合に、専用線３４の通信トラフィックに負荷がかかる可能性があるが、その負荷を分散するために以下のような構成を採用することもできる。

【００６２】例えば、利用者認証装置３０やサービス提供装置３２のCPU等の制御により、それらが送信する情報送信量等に一定の制限値を設けておき、情報送信量等がその制限値を越える場合には情報送信経由としてインターネット２６を選択させることによって専用線３４の通信トラフィックの負荷を分散させることができる。また、本実施形態においては示していないが、管理センター３８内のLAN３６と、専用線３４およびインターネット２６とを中継する複数のルーターを備えることによって、ルーター間で互いに遅延時間等をやり取りさせ、携帯電話２０に対する情報の送信を行う経路として、専用線３４またはインターネット２６のいずれが最適かを選択させることによって専用線３４の通信トラフィックの負荷を分散させることができる。これにより、携帯電話２０の利用者数が増加した場合にも、迅速かつ安定したシステムの運営が可能である。

【００６３】また、IPアドレスフィルタリング装置２８は、IPアドレスフィルタリングテーブルを備えているから、様々な仕様の携帯電話が新たに加わったり使用されなくなった場合に、IPアドレスフィルタリング装置２８が利用者認証装置３０に送信しない認証キーの設定や更新を行う際には、IPアドレスフィルタリングテーブルの記憶内容の更新のみで対応できる。

【００６４】ここで、IPアドレスは、変換装置２４にあらかじめプールされたものであり、コンピューターが管理・理解しやすい数字等によって表されるものであるから、IPアドレスフィルタリング装置２８に記憶させる内容の規格が統一化され、IPアドレスフィルタリングテーブルの記憶内容の更新が容易であるとともに、記憶容量を少なくすることができ、IPアドレスフィルタリング装置のフィルタリング処理を迅速化することができる。

【００６５】なお、本実施形態におけるIPアドレスフィルタリングテーブルには、Reject（禁止）するものの発信元のIPアドレスのカラムを記録しているが、これに限定されるものではない。例えば、Accept（送信する）のAction を指令するカラムや、あて先のIPアドレスのカラム、対象サービス（TCPポート番号）のカラムをこのテーブルに併せて記録してもよい。このようにした場合には、あて先のIPアドレスのカラムには、利用者認証装置３０やサービス提供装置３２内のサービス提供ウェブに割り当てられているIPアドレス等を、対象サービスのカラムには、httpやmail等のサービスの種類を記録することができる。

【００６６】なお、本実施形態においては、変換装置２４にルーター２９が設けられている場合を説明したが、ルーターを設けていない場合であっても本システムは実施可能である。なぜならば、この場合変換装置２４は、認証キーを専用線３４経由だけでなくインターネット２６経由にも送信することになるが、インターネット２６経由で認証キーを受けるIPアドレスフィルタリング装置２８は、上述したように、変換装置２４が付与するIPアドレスを含んだその認証キーを利用者認証装置３０に送信しないのであるから、結果として上記実施形態と同様の効果を奏することになるからである。

【００６７】（８）パーソナルコンピューター２１から利用者認証を受ける場合の処理

パーソナルコンピューター２１が利用者認証を受ける場合の構成では、図２に示すように、パーソナルコンピューター２１に接続された変換装置２３はインターネット２６のみに接続され、携帯電話２０の場合と違って専用線３４の経由による認証キーの送信はない。

【００６８】また、利用者認証のための識別子としては、IDとパスワードが要求されることが多い。これは、パーソナルコンピューターにはキーボードが通常備えられているから、利用者がIDやパスワードの入力を容易に行うことができる一方で、利用者認証をより確実に行うためである。

【００６９】パーソナルコンピューター２１から利用者認証を受ける場合の処理では、変換装置２３は、利用者端末が携帯電話である場合と同様に、認証キーを受けて、接続許可と認証キーに対するIPアドレスの付与、パーソナルコンピューター２１に対するIPアドレスの配布とを行う。そして、認証キーはプロトコル変換され、インターネット２６を介してIPアドレスフィルタリング装置２８に送信される。このとき、そのIPアドレスはIPアドレスフィルタリングテーブルに含まれているものと同一ではないから、LAN３６を介して利用者認証装置３０に送信されることになる。これは、すなわち、IPアドレスフィルタリング装置内のIPアドレスフィルタリングテーブルには、変換装置２４にプールされているIPアドレスが記録されており、一方の変換装置２３にプールされているIPアドレスが記録されていないのであるから、パーソナルコンピューターを発信元とする認証キーは、IP

アドレスフィルタリング装置２８による、送信しない（禁止）という動作の対象にならないことによるものである。

【００７０】このように、本実施形態においては、携帯電話２０が利用者端末の場合には専用線３４を経由して認証キーを送信等することによってなりすましによる不正利用を防止している一方で、パーソナルコンピューター２１が利用者端末の場合には専用線３４経由による認証キーの送信をしていない。これは、上記のように、携帯電話の場合は、利用者認証のために送信する認証キーが加入者IDやIPアドレスのように比較的偽造容易なものだからである。したがって、実施形態としてはこれに限られるものではない。例えば、使用される認証キーが偽造容易である等の事情により、なりすましによる不正利用がなされる懸念のあるその他の端末装置であっても、本実施形態における、携帯電話２０から利用者認証を受ける場合の構成と同様の構成を採用することにより不正利用を防止することができる。

【００７１】（９）IPアドレスフィルタリング装置２８のIPアドレスフィルタリングテーブルの記録内容を更新する場合の処理

図８に、IPアドレスフィルタリング装置２８のIPアドレスフィルタリングテーブルの記録内容を更新する場合の処理を示す。携帯電話２０から送信される電話番号に対して、変換装置２４が付与するIPアドレスが増えたり減ったりした等の更新があった場合には、変換装置２４のプールするIPアドレスが更新される（ステップＳ５０）。そして、変換装置２４のハードディスクのプログラムによって、更新されたIPアドレスのデータが専用線３４とLAN３６を介してIPアドレスフィルタリング装置２８に送信され（ステップＳ５１）、更新されたIPアドレスのデータを受信したIPアドレスフィルタリング装置２８は、IPアドレスフィルタリングテーブルの内容の更新を行う（ステップＳ５２）。

【００７２】したがって、IPアドレスフィルタリング装置２８が利用者認証装置３０に送信しない認証キーを、新たに設定する場合だけでなく、携帯電話の仕様が異なる様々なものが新たに加わったり減ったりした場合においても、IPアドレスフィルタリングテーブルの記憶内容の更新を簡易かつ迅速に行うことができる。

【００７３】また、更新されたIPアドレスのデータは、専用線３４とLAN３６のみを介してIPアドレスフィルタリング装置２８に送信されるから、データの安全性が確保される。すなわち、更新されたIPアドレスがインターネット２６上を流れた場合には、それを取得した第三者が不正利用端末２５を操作してそのデータに変更を加えたりする等することにより本システムが正常に機能しなくなるようにされるおそれがあるが、本実施形態によればそのような危険性はない。

【図面の簡単な説明】

【図１】従来の利用者認証システムを示す図である。

【図２】本発明の一実施形態による利用者認証システムを示す図である。

【図３】利用者端末としてのパーソナルコンピューターのハードウェア構成を示す図である。

【図４】IPアドレスフィルタリング装置のハードウェア構成を示す図である。

【図５】利用者端末としての携帯電話のブロック図を示す図である。

【図６】利用者認証を受ける場合の処理を示す図である。

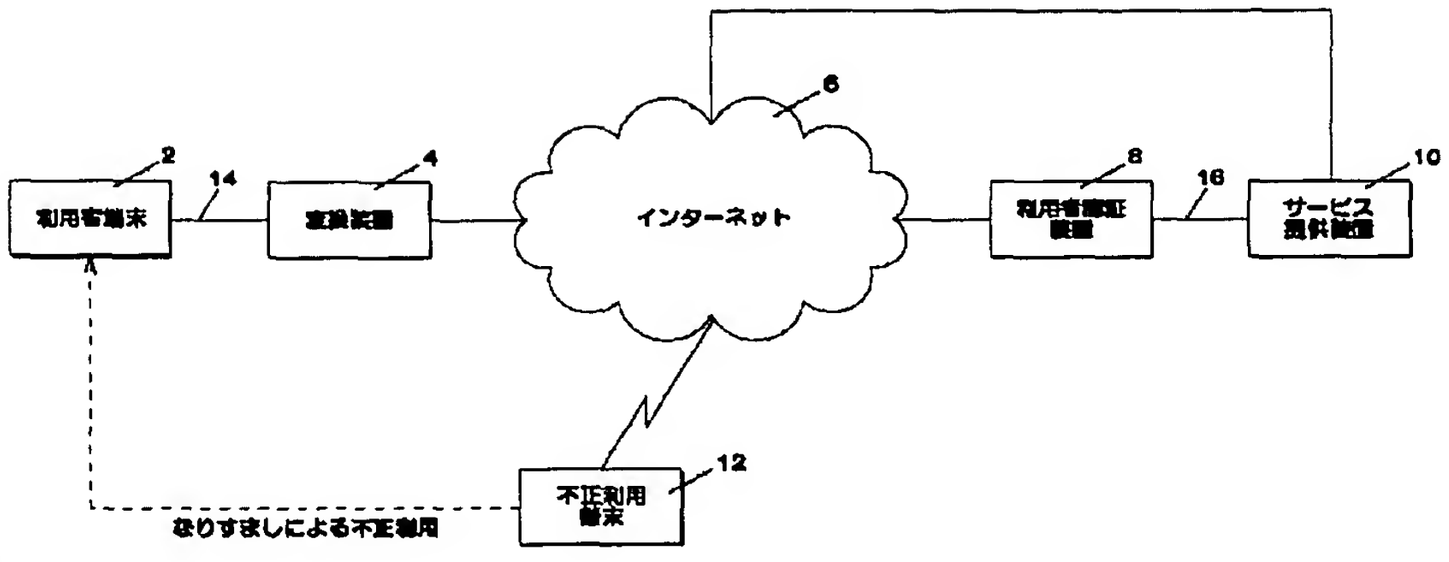
【図７】IPアドレスのフィルタリングテーブルの内容を示す図である。

【図８】IPアドレスフィルタリング装置のIPアドレスフィルタリングテーブルの記録内容を更新する場合の処理を示す図である。

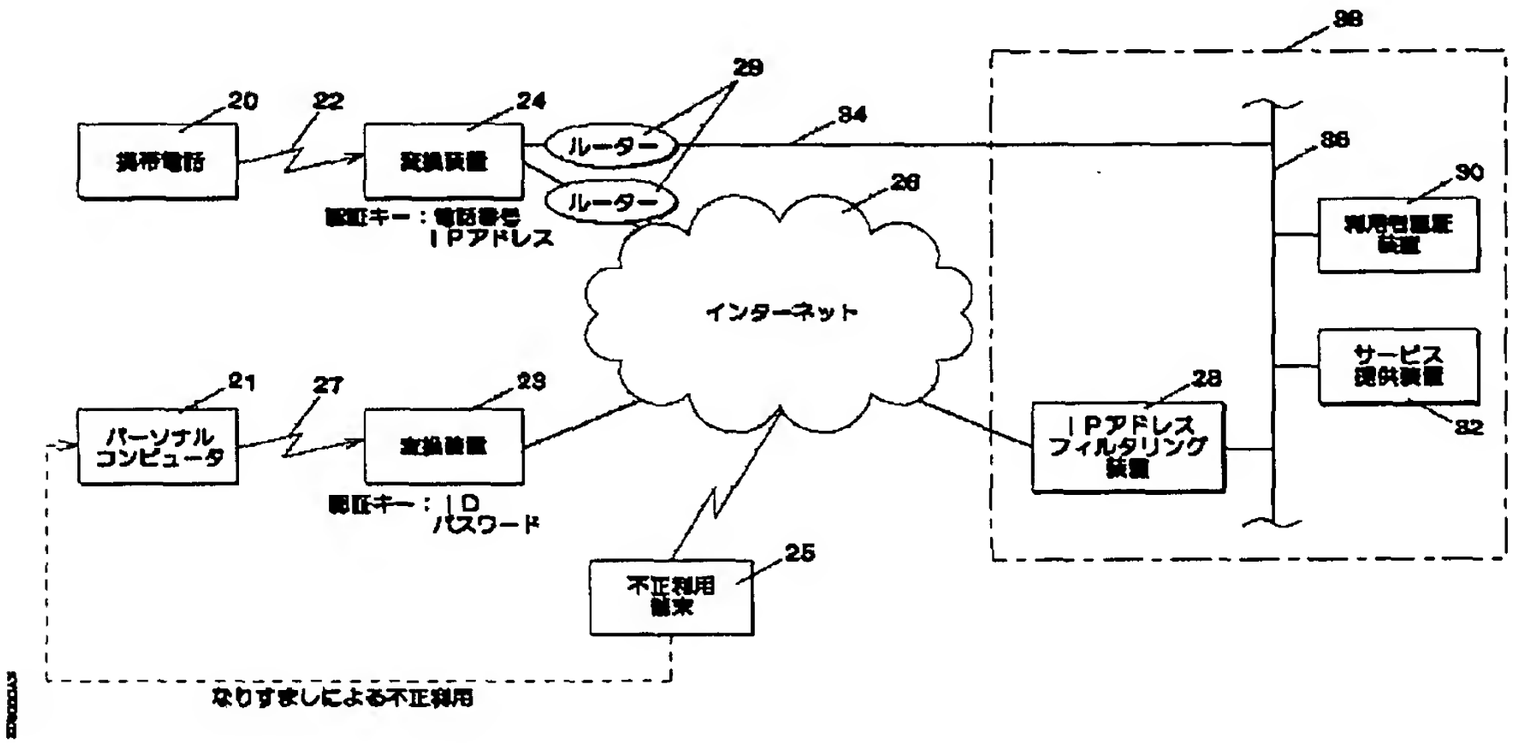
【符号の説明】

２０・・・携帯電話
２１・・・パーソナルコンピューター
２３、２４・・・変換装置
２８・・・IPアドレスフィルタリング装置
３０・・・利用者認証装置
３２・・・サービス提供装置
３８・・・管理センター
２９・・・ルーター
２２・・・電話網
２６・・・インターネット
３４・・・専用線
３６・・・LAN
２５・・・不正利用端末

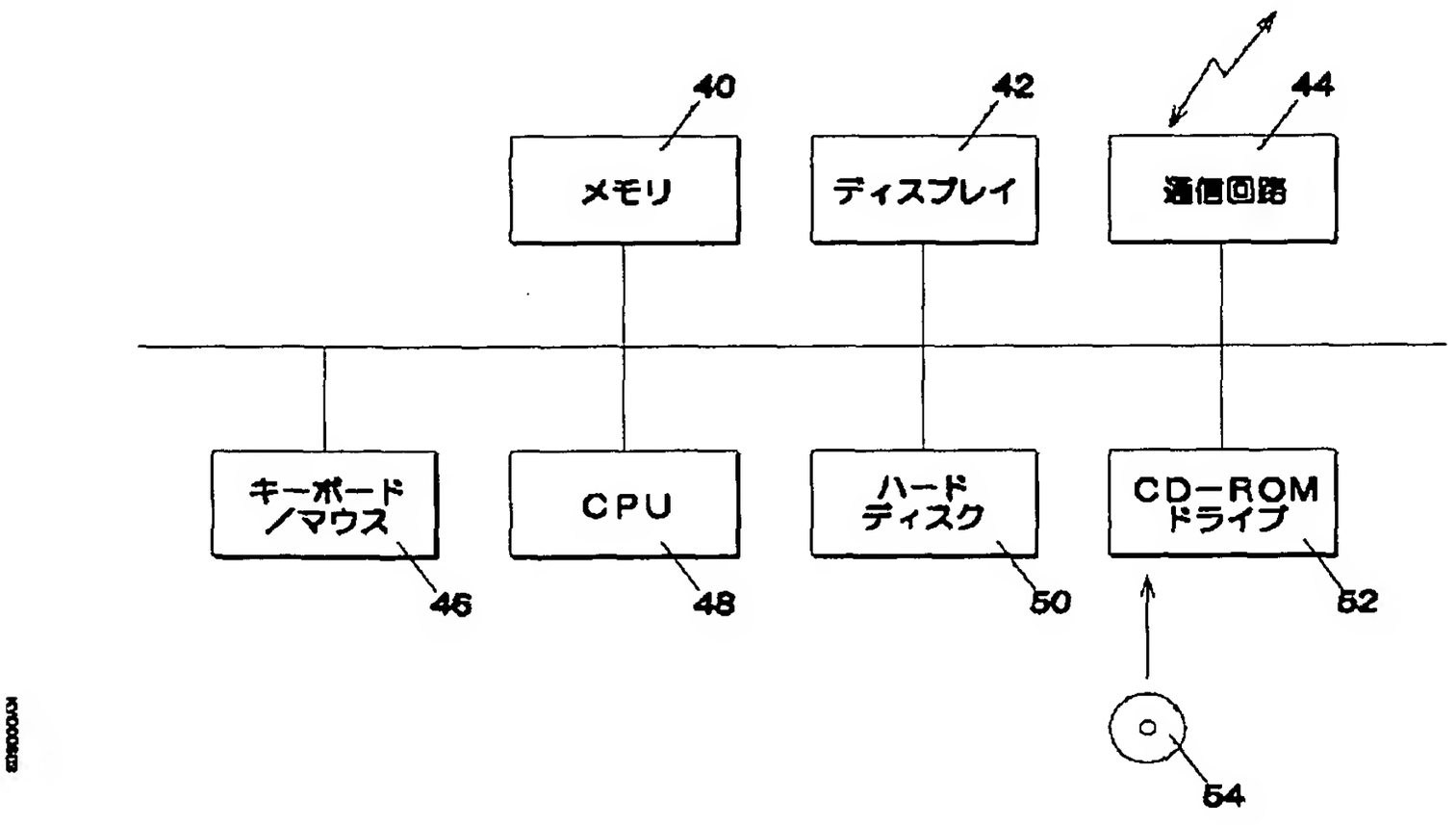
【図１】


2
14
4
6
8
16
10
利用者端末
変換装置
インターネット
利用者認証装置
サービス提供装置
12
不正利用端末
なりすましによる不正利用

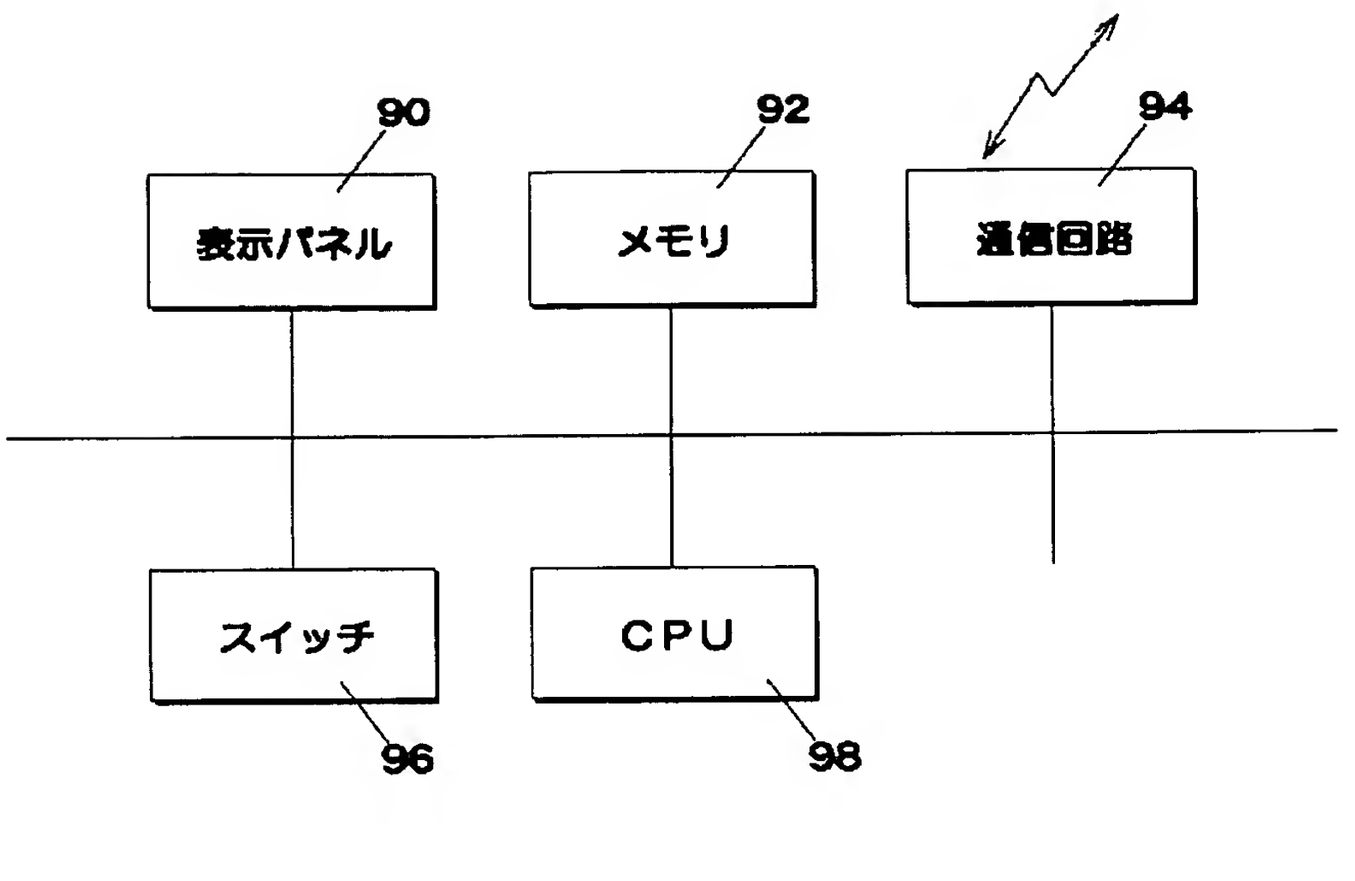
【図２】


38
20
22
24
29
34
36
30
携帯電話
変換装置
ルーター
ルーター
認証キー：電話番号
IPアドレス
26
インターネット
利用者認証装置
21
27
23
28
32
パーソナルコンピュータ
変換装置
IPアドレスフィルタリング装置
サービス提供装置
認証キー：ID
パスワード
25
不正利用端末
なりすましによる不正利用

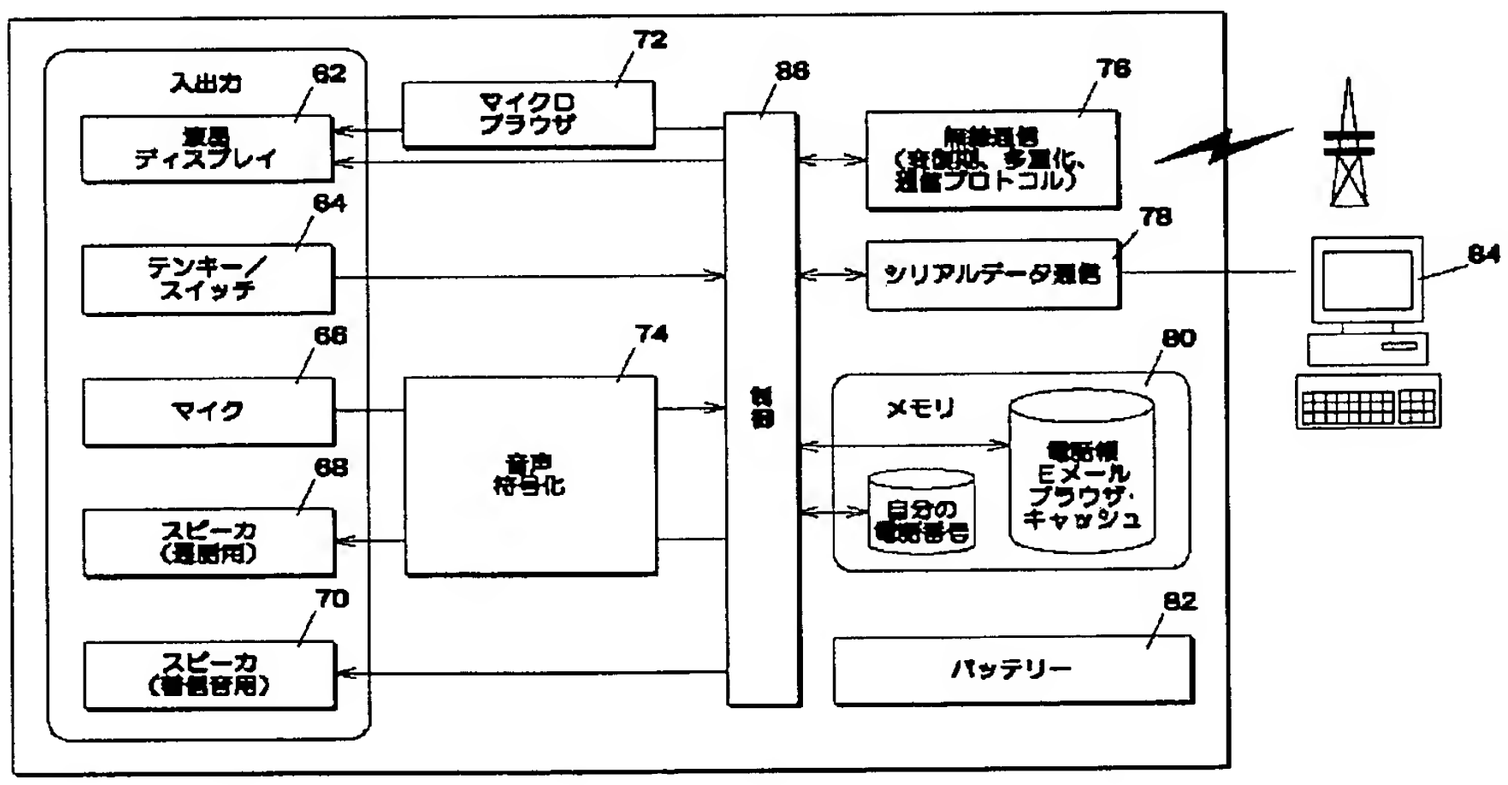
【図３】


40
42
44
メモリ
ディスプレイ
通信回路
キーボード／マウス
CPU
ハードディスク
CD－ROMドライブ
46
48
50
52
54

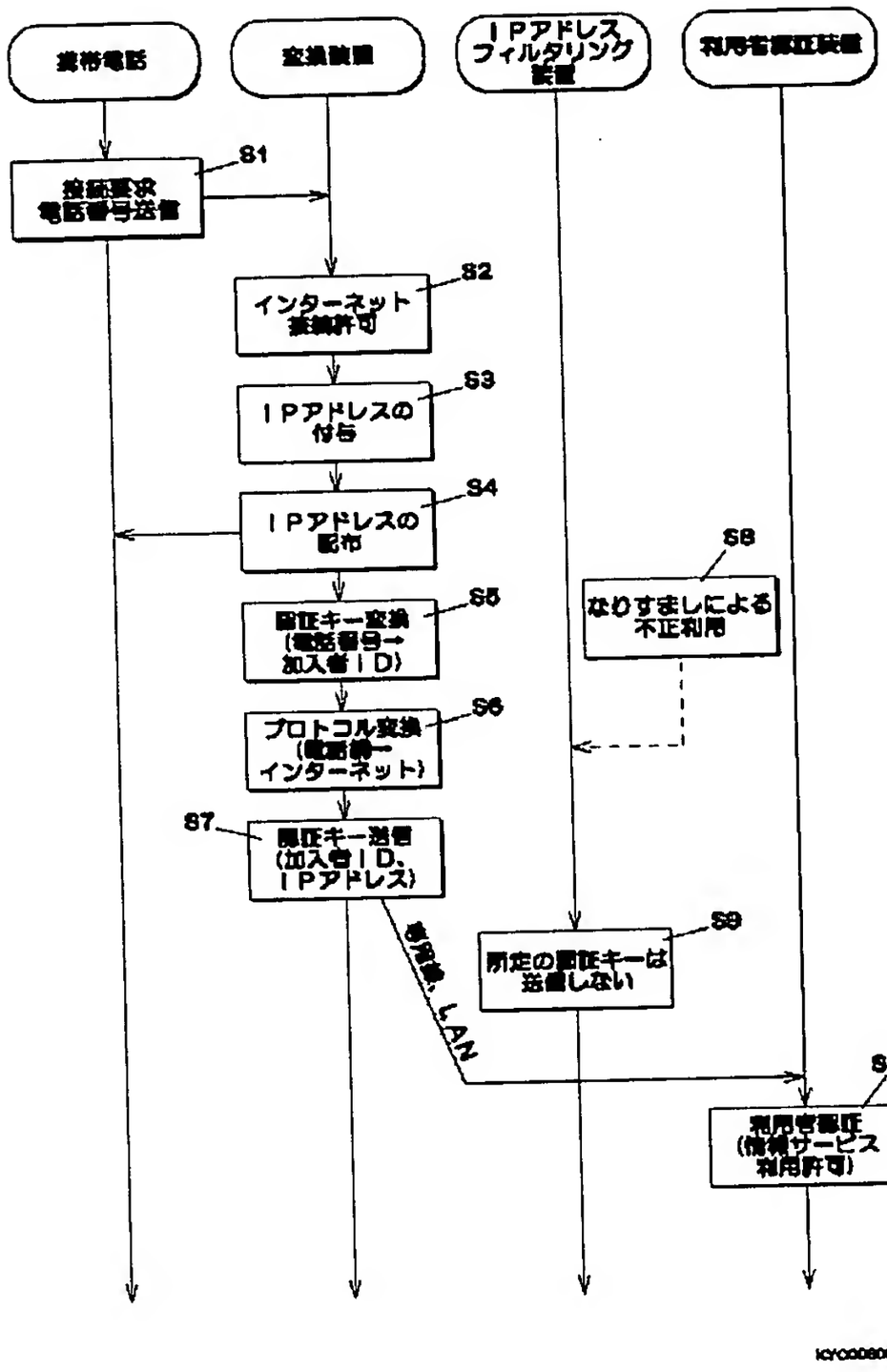
【図４】


90
92
94
表示パネル
メモリ
通信回路
スイッチ
CPU
96
98

【図５】


入出力
62
72
86
76
表示
ディスプレイ
マイクロ
ブラウザ
無線処理
（変調処、多重化、
通信プロトコル）
64
78
84
テンキー／
スイッチ
シリアルデータ通信
66
74
80
マイク
音声
符号化
制御
メモリ
電話帳
Eメール
ブラウザ、
キャッシュ
68
スピーカ
（通話用）
自分の
電話番号
70
82
スピーカ
（着信音用）
バッテリー

【図６】

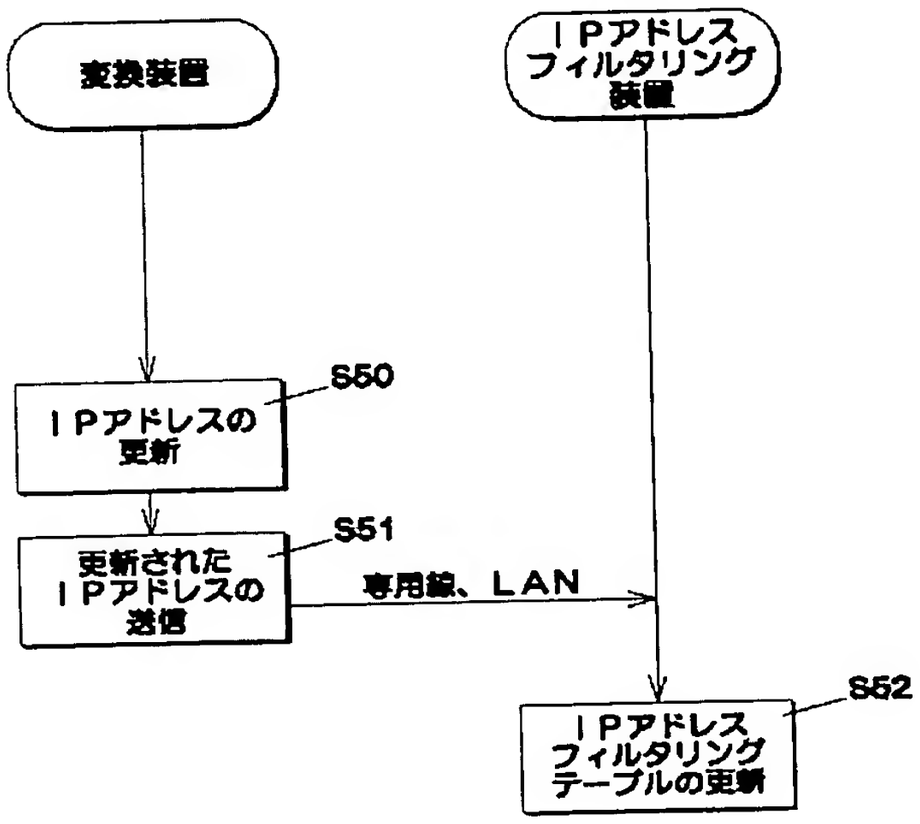


【図７】

Ａｃｔｉｏｎ＝Ｒ　ｊｅｃｔ（禁止） Ｓｏｕｒｃｅ（発信元のＩＰアドレス）
１９２．１６８．１．１ ～ １９２．１６８．１．２００
１９２．１６８．１０．１ ～ １９２．１６８．１０．５０
…．

KYC00607

【図８】



フロントページの続き

(72)発明者　大迫　哲郎
京都府京都市山科区東野北井ノ上町５番地
の22　京セラコミュニケーションシステム
株式会社内

Ｆターム(参考)　5B085 AE04 AE23 BG07
5J104 AA07 AA47 KA01 KA02 NA05
PA02 PA07
5K067 AA33 BB04 BB21 DD24 EE02
EE10 EE16 GG01 GG11 HH21
HH22 HH24